Deployables Check List
and
FAQ
(DCL-FAQ)

Final Version 1.4

12/21/04

Document Revision History

Table 1-1 Document Revision History

Version	Issue Date	Author/Modifier	Section, Page(s) and Text Revised
1.0	02/07/03	Julio Rivera	Original document
1.1	02/21/03	Julio Rivera	Added steps and minor revisions
1.2	01/20/04	Julio Rivera	Added new lessons/ Updated Flowcharts/ Minor revisions
1.21	01/28/04	Julio Rivera	Updated lesson # 32 OWA
1.22	03/24/04	Julio Rivera	Corrected typo in step #4 of the Deployment and step #10 of the Return
1.3	12/09/04	Jon Runyan	Renamed "Lessons Learned" section to "FAQ section". Modified doc title, file name and all other references.
1.3	12/09/04	Jon Runyan	Minor revisions to FAQs
1.3	12/09/04	Jon Runyan	Update Introduction section
1.3	12/09/04	Jon Runyan	Removed references to the Active Directory Security group in Checklist and FAQ.
1.4	12/21/04	Tim Phillips	Updated checklist and modify process chart as appropriate.

Change Request Form

Current Document Name: _____

Current Document Version/Date: _____

Name of Submitter:_____

Activity: _____

Phone/Email: _____

Your Voting Member Approval: _____

Date Submitted: _____

Title of Change: _____

Description of Change:

Reason for Change:

TO BE COMPLETED BY SPAWAR PMW-164   Date Received: _____

PMO Approve for Routing: _____ Date: _____

Valid Requirement: ☐ Yes   ☐ No Give Reason: _____

Forwarded for routing and approvals: Date Routed:_____
NMCI PMO Approval: _____ Date: _____

Approved as a revision to the document:
PMO: _____ Date: _____
New Document Revision: _____ Date Approved: _____
Revision Title: _____ Date Incorporated: _____

Contents

1   Introduction

This document provides amplifying information to assist the Unit IT in the deployment and return processes of the NMCI Deployable/Embarkable seats.
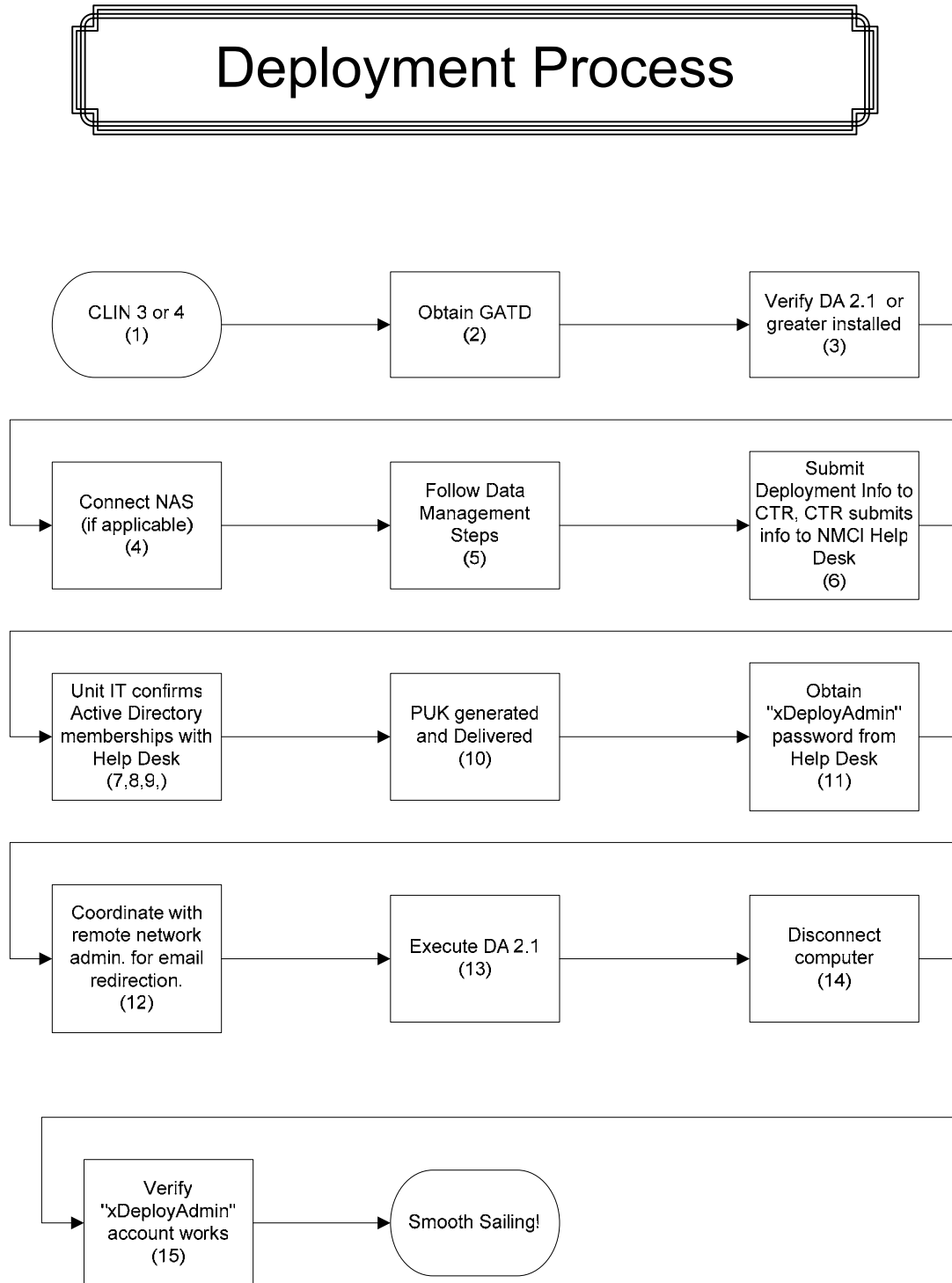
This document contains a set of summary checklists detailing the Deployables process and additional FAQs compiled during the development of the Deployable Architecture and the associated applications and processes. It is intended to be used as a supplement to the Government Aide to Deploy document, which provides the detailed step-by-step procedures that are used to deploy and return a seat.

The Checklist sections are intended to serve as an aid for those responsible for Deploying NMCI seats, providing a guide to help ensure Deployment goes smoothly. Included in each step of the checklist is a recommended timeframe for action.

The Frequently Asked Questions (FAQ) section is intended to help familiarize the reader with common problems and issues related to Deployables. The FAQ can be used to quickly get "up to speed" on certain regularly discussed topics.

2 Deployment Process

2.1 Deployment Process Flowchart

Deployment Process

```
CLIN 3 or 4          →     Obtain GATD        →     Verify DA 2.1 or
   (1)                        (2)                    greater installed
                                                          (3)

Connect NAS          →     Follow Data        →     Submit
(if applicable)            Management                Deployment Info to
   (4)                     Steps                     CTR, CTR submits
                           (5)                       info to NMCI Help
                                                     Desk
                                                     (6)

Unit IT confirms     →     PUK generated      →     Obtain
Active Directory           and Delivered            "xDeployAdmin"
memberships with           (10)                      password from
Help Desk                                            Help Desk
(7,8,9,)                                             (11)

Coordinate with      →     Execute DA 2.1     →     Disconnect
remote network             (13)                      computer
admin. for email                                     (14)
redirection.
(12)

Verify               →     Smooth Sailing!
"xDeployAdmin"
account works
(15)
```

2.2 Deployment Process Check List

The following table (2-1) provides a chronological list of items that should be performed prior to deployment in order to ensure a smooth evolution. It also provides references to the lessons learned which can be found in section 4 of this document.

Table 2-1 Deployment Process Check List

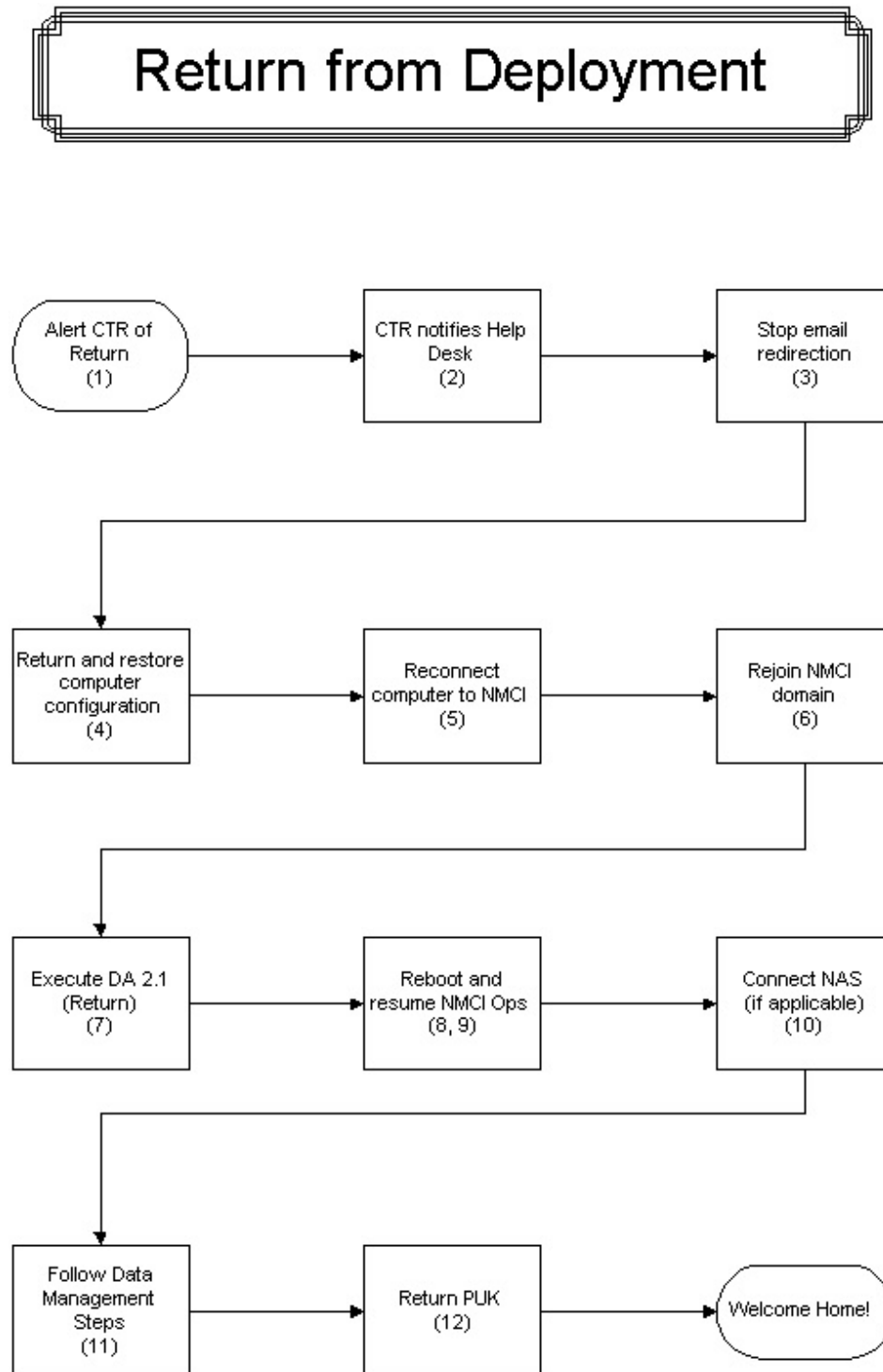| Check #	Recommended Days Prior to Movement	Check Off	Check Item	FAQ
1	NA	☐	Must have deployable CLIN 3-4	
2	21	☐	Obtain "Government Aide to Deploy" (GATD) document (V2.3 or later). Can be obtained from the Deployables Web Site: www.nmci.navy.mil Choose the "**Deployables**" link on the left-hand side. (u: deployer / pw: 4myusa!)	8,9
3	15	☐	Verify the application Deployables Architecture (DA) version 2.1 or greater is installed on the computer *a. C:\Program Files\Deployable Seat Application\ deployable.exe* b. If application is not present contact the Help Desk. c. If application is present open it, proceed to "Help" on the top menu and select "About"	3,4
4	14-21	☐	If applicable connect Network Attached Storage (NAS) to the NMCI network, in order to facilitate data transfer (CLIN 27 is needed). If NAS does not apply refer to Lessons Learned # 25 for alternatives.	27
5	10-14	☐	Follow data management procedures, which should be developed at the local or TYCOM level, to migrate data to the NAS or other devices as required.	27
6	10-14	☐	Unit IT submits "Request-to-Deploy" (AKA Embarkable MAC form) to local CTR , CTR submits info to NMCI Help Desk→ GATD, Section 2.0.1 →Form may be obtained from: www.nmci.navy.mil Choose the "**Deployables**" link on the left-hand side. (u: deployer / pw: 4myusa!)	

Check #	Recommended Days Prior to Movement	Check Off	Check Item	FAQ
7	10-14	☐	Help Desk verifies unit IT is in the "Unit IT Security Group" → GATD, Section 2.0.1	5
8	10-14	☐	Help Desk verifies that computer is in the "Deployables software group" → GATD, Section 2.0.1	5
9	10-14	☐	Recommend Unit IT coordinates with Help Desk to verify steps 7-9 by calling Help Desk directly. a. Unit IT must maintain and track configuration changes to all computers in order to facilitate the return process → GATD, Section 2 b. Unit IT must generate and maintain a listing of assets and users → GATD, Section 2.0.5. **Note:** Maintain list of port numbers. All computers must be reconnected to their original ports in order to avoid a port lock-out where port security is active.	6,8 25,26,
10	3-10	☐	The PUK is generated and delivered by the local Base Ops to unit IT as a result of the "Request-to-Deploy" submitted. If PUK is not delivered within three days of unit movement contact the NMCI Help Desk and open a trouble ticket. If that effort fails to produce results the ISF Deployables ILS Manager may be contacted <u>as a last resort only</u>: Theo Halstead, e-mail: theadore.halstead-eds@eds.com, Office: 619-817-3582, Cell: 760-473-4115. → GATD, Section 2.0.1	10, 11 12, 13 14,15, 19, 20
11	0-3	☐	Unit IT will call the Help Desk and obtain the current "xDeployAdmin" password. **Note**: Password changes every month, but not for seats already deployed. → GATD, Section 2.0.1	17

Check #	Recommended Days Prior to Movement	Check Off	Check Item	FAQ
12	1-3	☐	Users/unit IT redirects e-mail → GATD, Section 2.0.2 a. Redirect from within NMCI or via RAS from the following website: https://deployables2. If user does not have access to the website he/she can contact the Help Desk directly via telephone or e-mail and request e-mail redirection.	**28, 29 30, 31**
13	1-3	☐	Users/unit IT execute DA 2.1 application (Deploy) → GATD, Section 2.0.2	**7, 16**
14	0-3	☐	Users/unit IT disconnect computer	
15	0-3	☐	Unit IT verifies "xDeployAdmin" account works with provided password and ensure it is a member of the "Administrator" group	**18**

3   Return Process

3.1   Return Process Flowchart

Return from Deployment

```
Alert CTR of         →    CTR notifies Help    →    Stop email
Return                    Desk                      redirection
(1)                       (2)                       (3)
                                                        │
                                                        ▼
Return and restore   →    Reconnect            →    Rejoin NMCI
computer                  computer to NMCI          domain
configuration             (5)                       (6)
(4)                                                     │
                                                        ▼
Execute DA 2.1       →    Reboot and           →    Connect NAS
(Return)                  resume NMCI Ops           (if applicable)
(7)                       (8, 9)                    (10)
                                                        │
                                                        ▼
Follow Data          →    Return PUK           →    Welcome Home!
Management                (12)
Steps
(11)
```

3.2   Return Process Check List

The following table (3-1) provides a chronological list of items that should be performed prior to return from deployment. It also provides amplifying references to the lessons learned which can be found in section 4 of this document.

Table 3-1 Deployment Process Check List

Check #	Recommended Days Prior to Movement	Check Off	Check Item	LL
1	10	☐	Unit IT submits "Request-to-Return" (AKA Embarkable MAC form) to local CTR → GATD, Section 2.2.1 → Most likely the form will contain the same information as the "Request-to-Deploy" submitted during the Deployment process. →Form may be obtain from http://www.nmci-isf.com/helpdesk_reqforms.htm.	
2	10	☐	Local CTR enters request into e-forms or e-mails Help Desk → GATD, Section 2.2.1	
3	2-1	☐	Stop e-mail redirection before departing remote network → GATD, Section 2.2.3	
4	0	☐	Users/unit IT physically returns and restore original computer configuration prior to connecting the computer to the NMCI environment → GATD, Section 2.1, 2.2.2, 2.2.5, 2.2.6	**23, 24 25, 26**
5	0	☐	User/Unit IT reconnects the computer to its original NMCI port.	
6	0	☐	If another domain was joined while deployed, unit IT rejoins NMCI domain → GATD, Section 2.2.4	
7	0	☐	Users/unit IT executes DA 2.1 application (Return) → GATD, Section 2.2.7	**7**
8	0	☐	Reboot computer one final time to initialize NMCI services	

9	0	☐	Resume Normal NMCI operations	
10	0- +21	☐	If applicable connect Network Attached Storage (NAS) to the NMCI network, in order to facilitate data transfer from the NAS to NMCI.	27
11	0- +21	☐	Follow data management procedures, which should be developed at the local or TYCOM level, to migrate data from the NAS (or other devices) to NMCI as required.	27
12	+14	☐	Return PUK to local ISF Site Delivery Manager or contact Help Desk within two weeks.	

4   FAQ section

1. **What is the DA version 2.1 (or above) application?**

   The Deployables Architecture (DA) application V. 2.1 is a program that automates the process of removing a computer from the NMCI environment and subsequently returning it to NMCI. It allows a Unit IT to have administrative control over the seat to perform a variety of IT functions such as change domains and install applications.

2. **What exactly does the DA 2.1 do?**
   * It creates the account "xDeployAdmin" on the local computer
   * It assigns the "xDeployAdmin" account to the Administrators Group
   * It generates a password for the "xDeployAdmin" account based on the current month
   * It changes the password on the "xAdministrator" account (ISF's access account)
   * It disables all instances of the Enterprise Management System (EMS) software, such as Tivoli and Radia.
   * The process is reversed upon return

3. **How do I check the deployable application and the version?**
   * Find the application under the "Start/Deployable Seat Application" menu or use Windows explorer to navigate to the following location: 'C:\Program Files\Deployable Seat Application\ deployable.exe'
   * Open the application by double clicking it
   * Proceed to "Help" and then "About"
   * The correct version is 2.1.1 or higher.

4. **What if I have no application or the wrong version loaded on my computer?**

   Although NMCI advertises that all Deployable computers will be automatically loaded with the proper application, it is best to ensure you do have it by following the steps listed in question # 3. Otherwise:

   * Contact the Help Desk.
     o If Help Desk does not respond in a timely manner contact your CTR.

5. What are security groups?

NMCI assigns Unit IT' to the "Unit IT Security Group." Only a user assigned to the "Unit IT Group" will receive the Xdeployadmin password from the Help Desk and can rejoin the NMCI domain, if another domain was joined while deployed. The actual group names are:

- Domain: NADSUSEA
- Unit IT Group: W-NAEA-DEP_ITREP-GS01

- Domain: NADSUSWE
- Unit IT Group: W-NAWE-DEP_ITREP-GS01

6. How can I check if I am in the "Unit IT Security Group?"

Although NMCI advertises that Unit IT Deployable users will be assigned to the proper groups, it is best to call the Help Desk and ensure you are in the group listed in question # 5.

7. What if I receive an error message when attempting to deploy the computer that says:

Application Server Connection Error

Unable to connect to Deployable Application Server. Ensure the computer is part of the NMCI Domain, connected to the NMCI network and the user account is part of the Deployables Security Group.

OK

- This error message indicates possibly some conductivity problems with NMCI back to the Deployable Server. Contact the Help Desk to notify the problem.
- Another possible source for message is a loose network connection cable behind your seat. Please verify it if you have been relocation you seat during deployment.

8. What is the Government Aide to Deploy (GATD) document?

The document is a detailed set of instructions intended to help the Unit IT support the NMCI Deployable process.

9. How do I get a copy of the Government Aide to Deploy document?

The latest version can be obtained directly from the "Deployables Website" at
http://www.nmci.navy.mil/Primary_Areas/Deployables-Embarkables/Deployables_Embarkables;
to gain access to website use "deployer" and "4myusa!" as user name and password correspondingly (Note: user-name and password are all lower case).

10. What is a Pack-up-Kit (PUK)?

The PUK is a logistic package intended to provide the Unit IT the ability to be self sufficient and support NMCI Deployables while on deployment. The PUK contains the GATD document, spare equipment, the Break-Fix document, and the CD media used to re-image a system.

11. Where can I find more information about the PUK?

More PUK information can be obtained directly from the Deployable Break Fix Support document at the "Deployables Website" via http://www.nmci.navy.mil/Primary_Areas/Deployables-Embarkables/Deployables_Embarkables; to gain access to website use "deployer" and "4myusa!" as user name and password correspondingly (Note: user-name and password are all lower case).   .

12. What is the Deployable Break Fix Support document?

The Deployable Break Fix Support document gives the Unit IT the ability to achieve and sustain self-sufficiency while in a deployed status by providing detailed instructions on how to use the PUK in order to repair, rebuild, or replace the deployable seats. It also provides guidance on how to arrive at a reasonable number of replacements that should be included in the PUK.

13. What are the contents of the PUK?
- A copy of the NMCI standard image: "Gold Disc"
- A copy of the DA 2.1 or higher
- A copy of all the approved applications for that particular unit (Approved Legacy Apps)
- A copy of the PAL software (RAS)
- A copy of the VPN software (RAS)
- Spare computers
- A copy of the Government Aide to Deploy document
- A copy of the BIOS password

14. How do I get a PUK?

The PUK is generated when the local CTR submits the "Request-to-Deploy" (AKA Embarkable MAC) to the NMCI Help Desk in response to a request from the Unit IT.   The Help Desk will then open a ticket and forward it to the local Base Ops for action. EDS personnel should then deliver the PUK within three days of the actual deployment day. In some cases where the movement is immediate and EDS can not support the rapid deployment, the PUK will be FedEx to the final destination; if commercial shipping is not available at final destination USN supply channels will be used for final delivery. Refer to the GATD, section 2.0.1.

NOTE: Submitting deployment information early will ensure that the PUK is delivered in a timely manner.

15. How do I refresh the PUK while deployed?

To refresh the PUK the Unit IT must contact the Help Desk, via phone or e-mail, and inform them of the requirements. Refer to the GATD, section 2.3.2.

16. What can I do if I deploy without executing the DA 2.1?

If this occurs there several options:

- RAS back to NMCI and execute the DA 2.1
- Contact the Help Desk
- Reload the Gold Disc (Refer to <u>Deployable Break Fix Support</u> document, Section 3.4)
    - o Data must be backed up before loading Gold Disc
    - o Seat will not be in deployed status; NMCI Help Desk must be contacted first upon return.

17. How can I get the "xDeployAdmin" password?

The password can be obtained by calling the Help Desk. Refer to the GATD, section 2.0.1. **Note**: Only the Unit IT or designated POC will be given the password via e-mail. Only in special circumstances, as determined by the Help Desk, will the password be given over the phone. Please notify the Help Desk agent if you do not have access to your NMCI e-mail, or a military or government e-mail address where you have re-directed your NMCI e-mail.

18. What if I receive the wrong "xDeployAdmin"password?

Passwords are assigned based on the current month. Once the password is generated by the DA 2.1 it does not expire. However it is possible to have multiple passwords within a unit, if the actual deployment occurs at the end/beginning of the month.

If a user attempts to log on with the wrong "xDeployAdmin" password three times in a row, the system will lock out the account for 30 minutes. The user can reset the account before 30 minutes have elapsed by using the normal NMCI account login and returning the computer from deployment using DA 2.1 (NMCI connectivity is required). The user should then reboot the computer and deploy again using DA 2.1.

Before attempting to log in again using the "xDeployAdmin" account the user should contact the Help Desk to obtain the correct password.

19. Why do I need a BIOS password?

If it becomes necessary to reload the computer with the Gold Disc or perform any advance function on the computer the BIOS password will be needed. NMCI locks the BIOS from the users and it sets the boot sequence to hard drive only.

20. How do I get the BIOS password?

The BIOS password is provided as part of the PUK.

21. When should I reload the Gold Disc?

NOTE: Reloading the Gold Disc will permanently delete all data. IF POSSIBLE BACK UP YOUR DATA BEFORE LOADING THE GOLD DISC.

The Gold Disc should be reloaded under the following circumstances:

- Last resort if administrator rights have not been granted, due to not using DA 2.1 (see question 16)
- If software becomes corrupt beyond repair

Note: The DA 2.1 (or higher) back up floppy will be needed during this procedure. If the floppy is not available DO NOT USE THE FLOPPY FROM A DIFFERENT COMPUTER. Each computer must have its own back up floppy created on that particular computer.

Also during the reloading of the Gold Disc the user will be prompted to enter a computer name; this name must be the exact NMCI assigned name that the computer originally had. If these procedures are not followed a Move/Add/Change (MAC) charge may result. Refer to GATD, Section 2.0.5 and

22. What are the default NMCI TCP/IP settings?

NMCI computers are normally set to DHCP.

23. Can I change the TCP/IP settings?

The Unit IT may change anything on the computers that he/she sees necessary while deployed. However, the Unit IT is responsible to return the computer to its original configuration before it is reintegrated into the NMCI network. Refer to GATD, Section 2.1

24. What are the network card settings for NMCI?

Most NMCI computers are set to auto sensing, and some are set to 100Mb, Full Duplex. These settings may also be changed at the Unit IT's discretion if required to join another domain. However, the Unit IT is responsible to return the computer to its original configuration before it is reintegrated into the NMCI network. Refer to GATD, Section 2.1

To change the network card settings follow these instructions (Unit IT must log on as "XdeployAdmin"):

a. Right clik on "My Network Places" and select "Properties"
b. Double click on "Local Area Connection"
c. Select the "Configure" button on the new window
d. Select "Advanced" tab at the top of the new window
e. Select "Media Type" under the "Property" text box
f. Select setting desired from the "Value" pull-down menu
g. Restart computer

25. What is Port Security?

Port Security refers to the NMCI feature where the network wall-jack or port is configured to only accept a specific computer. This is accomplished by reading the Media Access Control (MAC) address of the network card.

Note: If you have a docking station the MAC address recorded by NMCI will be that of the network card built into the docking station and not the MAC of the laptop.

26. Why must I know about Port Security?

Port Security is enabled on some NMCI bases. This prevents users from moving theirs computers around, even from one wall-jack to another within the same outlet. If the wrong computer is connected to the wall-jack, the port will shut down. It will be necessary to contact the Help Desk, and may be the local ISF representative, in order to reactivate the port. Unit IT's should maintain an active inventory of their assets, including port numbers.

27. When do I back up my data?

Each Unit IT should develop a comprehensive data back-up plan. Data should be backed-up before leaving the NMCI network, during the deployment, and upon return to the NMCI network. There are several ways to back up data. However, not all are part of the standard NMCI Deployable seat; additional charges may apply.

- GFE Network Attached Storage (Must be certified and a CLIN 27 must ordered)
- NMCI Network Drives (700 MB per user)
- Floppy Disk
- CDR-W
- Zip Disk
- Jazz Disk
- USB Removable Hard Drive

Note: It is the responsibility of each user to safe guard and back-up their data.

28. When do I redirect my e-mail?

E-mail redirection should be done the day of movement or the "Pack-up" day, whichever fits the user's schedule.

29. How do I redirect my e-mail?

The user must log on to any NMCI computer and go to 'https://deployables2' or contact the Helpdesk while deployed.

Refer to GATD, Section 2.0.2.

30. Can I redirect e-mail through RAS?

Yes, establish a RAS connection and proceed to 'https://deployables2'

Refer to GATD, Section 2.0.2.

31. Do I have to redirect e-mail?

No, if a user will not be joining another domain and will have access to a phone line, then RAS can be used to read e-mail. Also Outlook Web Access (OWA) can be accessed from any computer with an Internet connection, Internet Explorer 6.0 or higher, 128-bit encryption on the browser, and the user's PKI certificate.

32. What is Outlook Web Access (OWA)?

OWA is a web based Exchange client that allows users to have full access to their NMCI e-mail and Exchange public folders. The following requirements apply:

- Any computer with an Internet connection
- Internet Explorer 5.0 or higher
- 128-bit encryption on the browser
- User's PKI certificate loaded on the computer

The address to OWA is 'https://webmail.navy.mil'

For further information please read the OWA Reference Guide, which can be found at the following link: http://www.nmci-isf.com/downloads/userinfo/OWAQRG.pdf

33. How do I get a PKI certificate?

PKI soft certificates are not longer issue by EDS. PKI certificates are contained within the CAD Card.

34. Does NMCI use Proxy settings on their browser?

Yes, these settings must be recorded and changed by the Unit IT before connecting to another network. Web surfing will not likely work on another network unless these settings are removed or changed.

35. Can I redirect my e-mail while Outlook is running?

No, the user will receive an error if he/she attempts to redirect the e-mail while Outlook is running. However, after the e-mail is redirected the user can open Outlook and work normally, with the exception that e-mail will not be received at that address.

36. How do I update my anti-virus software and implement Information Assurance Vulnerability Alert (IAVA) updates?

37. How do I avoid deletion of the user's locally cache profiles, including "My Documents" files, upon returning to NMCI domain from ISNS Networks?

It has been discovered that the ISNS or IT-21 environment installs a registry entry on the NMCI computers which causes the active profile to be deleted from the local hard drive when the user logs off. To solve this problem, a patch has been developed which resets this setting in the Registry. The patch can be found in the deployables website; http://www.nmci.navy.mil/Primary_Areas/Deployables-

Embarkables/Deployables_Embarkables, use "deployer" and "4myusa!" as user name and password respectively.

Once the patch is downloaded double click on the file and follow the prompts.
Note: This action must be performed before rejoining the NMCI domain to avoid deletion.

38. Can I use High-speed RAS/Broadband connectivity with my NMCI deployable seat?

At this time high-speed broadband connectivity is not available for NMCI seats. However, negotiations are ongoing to add this capability to the NMCI contract.

39. Can I call the NMCI Help Desk using a DSN line?

Yes, the DSN number to the NMCI Help Desk is 577-HELP. It works exactly the same as the regular NMCI Help Desk number, 1-866-THE-NMCI.

40. Can I RAS from my NMCI Deployable seat using a DSN line?

Yes, a user must have the following:
- RAS enabled on his/her NMCI account
- His/her PKI cert loaded on the computer or have the floppy with the cert in order to load it
Once the user has the above items in place he/she can then use the NMCI DSN RAS number to establish connectivity. The NMCI DSN RAS number is 524-7009.